APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/578,087	05/03/2006	Mauro Sentinelli	09952.0033	4710

22852   7590   02/02/2010
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER
ZIA, SYED

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
02/02/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/578,087	SENTINELLI, MAURO
	Examiner	Art Unit	
	SYED ZIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>23 November 2009</u>.

2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>33-51 and 53-62</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>33-51 and 53-62</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to amendment and remarks filed on November 23, 2009.

The amendments filed on November 23, 2009 have been entered and made of record. Claims 33-
51 and 53-62 are pending.

Claim Rejections - 35 USC § 101

1.   Previous rejection under 35 U.S.C. 101 has been withdrawn

Claim Objections

Applicant cancelled the Claim 52 making previous objection moot.

Response to Arguments

Applicant's arguments filed on November 23, 2009 have been fully considered but they

are not persuasive because of the following reasons:

Regarding Claims 33-51 and 53-62 applicants argued that the cited prior arts (CPA) [Alie

(U. S. Publication No.: 2003/0055738)] specifically, does not disclose or suggest at least

Applicant's claimed "*performing a first, SIM-based authentication of the user's data processing*

terminal in the data processing system at an authentication data processing server" and

"*conditioning the authentication of the user's data processing terminal in the data processing*

system to a second authentication," as recited in independent claims.

Applicant further argued that although Alie discloses that SIM-based applets can be used to

implement the system, the SIM in Alie's system is only provided in the mobile handset, and there

is still only one authentication process between the server and the mobile handset.

In contrast, Applicant's claim 33 recites "*performing a first, SIM-based authentication of the*

user's data processing terminal in the data processing system at an authentication data

processing server" and "*conditioning the authentication of the user's data processing terminal in*

the data processing system to a second authentication".

This is not found persuasive. The system of cited prior art teaches mobile transaction

device that has smart card with encryption keys and calculates response using ID code,

transaction value and challenge. This personal mobile device comprises means for receiving

information related to a transaction and sending a response, a hardware secure module (smart

card) with encryption keys for processing information and calculating the response, an interface

for displaying information and prompting the end user for the identification code (PIN) and

means for inputting the identification code and approving the transaction. The transaction

information includes a challenge value, a label containing context information and a numerical

value.

Specifically, the present invention consists of a system and method for effecting

transactions with strong multi-factor end user authentication, using personal mobile devices.

This system includes the authentication server side processing of the transaction request. The authentication server sends the request information to its own HSM to obtain a derived challenge value (a non-predictable number) which is attached to a label containing context information as well as a numerical value pertaining to the transaction (transaction value, transaction number, or other), so that the transaction is uniquely identified

This system further consists of the procedure implemented by the personal mobile device (e.g. a personal digital assistant or a mobile handset), including its own HSM, to calculate and send back a response (signature).At the personal mobile device, the elements sent by the server are transferred to and processed by the HSM. If the personal mobile device has a direct connection, e.g. through a wireless link, to the server then the transfer of all elements is automatic. If it has an indirect connection, for example the information is shown on a personal computer display, the user must manually transfer two of the three elements (i.e. the challenge and the transactional value) using the personal mobile device input capability. The personal mobile device displays the information relating to the transaction, such as the value, and prompts the person for a PIN. The HSM uses the PIN, the transaction value, the challenge, and encryption keys to calculate a response. The response is sent to the server, automatically or manually depending on the type of the connection with the server ([Fig.2-7, and 0010-0018, 0048-0041, and 0070-0096]).

As a result, cited prior art does implement and teach a system that methods that relates to authenticating users of data processing systems using SIM based authentication involving an exchange of identification data stored on a Subscriber Identity Module.

Applicants <u>clearly</u> have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent Claims and in subsequent dependent Claims. Accordingly, rejections for claims 33-51 and 53-62 are respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 33-62 are rejected under 35 U.S.C. 102(b) as being anticipated by Alie (U. S. Publication No.: 2003/0055738).

1.   Regarding Claim 33 Alie teaches and describes a method of authenticating a data processing terminal of a user for granting the data processing terminal access to selected services provided by a data processing system, the user being provided with an authenticatable mobile communication terminal adapted to be used in a mobile communication network, comprising:

performing a first, SIM-based authentication of the user's data processing terminal in the data

processing system at an authentication data processing server, said performing the SIM-based

authentication comprising operatively associating with the user's data processing terminal a first

subscriber identity module issued to the data processing terminal user; having the user's mobile

communication terminal authenticated in the mobile communication network; and conditioning

the authentication of the user's data processing terminal in the data processing system to a second

authentication, said second authentication being based on identification information provided to

the user at the mobile communication terminal through the mobile communication network

([0070-0096]).

2.   Regarding Claim 44 Alie teaches and describes a method by which a data processing

terminal in a data processing system is authenticated in order to be granted access to selected

services provided by the data processing system, the method comprising: interacting with a first

user's subscriber identity module (SIM) operatively associated with the data processing terminal,

and with an authentication data processing server in the data processing system, for performing a

SIM-based authentication of the user's data processing terminal; acquiring personal identification

information provided to the user at a user's mobile communication terminal for second

authentication, wherein the second authentication is through a mobile communication network;

and sending said personal identification information to the authentication data processing server

for completing the authentication of the data processing terminal ([0070-0096]).

3.   Regarding Claim 48 Alie teaches and describes a method by which an authentication data processing server authenticates a user's data processing terminal in a data processing system in order to grant the data processing terminal access to selected services provided by the data processing system, comprising: receiving a request of authentication of the data processing terminal, the data processing terminal having operatively associated therewith a first subscriber identity module; performing a SIM-based authentication of the data processing terminal based on data associated with the first subscriber identity module; providing the user with first personal identification information by exploiting a user's mobile communication terminal authenticated in a mobile communication network; and conditioning the authentication of the user's data processing terminal to a prescribed correspondence between the first personal identification information provided to the user and second personal identification information received from the user's data processing terminal in reply to the provision of the first personal identification information ([0070-0096]).

4.   Regarding Claim 53 Alie teaches and describes in a data processing system, a system for authenticating a data processing terminal of a user so as to grant the data processing terminal access to selected services provided by the data processing system, the user having an authenticatable mobile communication terminal adapted to be used in a mobile communication network, comprising: a first subscriber identity module operatively associatable with the data processing terminal; and an authentication data processing server adapted to carry out a first authentication step based on the first subscriber identity module; the authentication data processing server being further adapted to carry out a second authentication process based on

identification information provided to the user at the mobile communication terminal through the mobile communication network ([0070-0096]).

5.   Regarding Claim 60 Alie teaches and describes an authentication kit for authenticating a user's data processing terminal in a data processing system in order to grant the data processing terminal access to selected services provided by the data processing system, comprising: a first subscriber identity module; a computer peripheral device having associated therewith the first subscriber identity module and operatively associatable with the user's data processing terminal; and a second subscriber identity module operatively associated with a user's mobile communication terminal for allowing connection thereof to a mobile communication network ([0070-0096]).

6.   Regarding Claim 62 Alie teaches and describes an authentication kit for authenticating a user's data processing terminal in a data processing system in order to grant the data processing terminal access to selected services provided by the data processing system, comprising: a first subscriber identity module; a computer peripheral device having associated therewith the first subscriber identity module and operatively associatable with the user's data processing terminal; a second subscriber identity module operatively associated with a user's mobile communication terminal for allowing connection thereof to a mobile communication network; and the computer program product of claim 47 or 51 ([0070-0096]).

4.   Claims 34-43, 45-47, 49-52, 54-59, , and 61 are rejected applied as above rejecting

Claims 33, 44, 48, 53, and 60. Furthermore, Alie teaches and describes data dependent

scrambler, wherein:

As per Claim 34, said second authentication comprises: generating a first password at the

authentication data processing server; sending the first password to the mobile communication

terminal over the mobile communication network; and checking a correspondence between the

first password and a second password, depending on the first password, entered at the data

processing terminal and provided to the authentication data processing server through the data

processing system ([0058-0068]).

As per Claim 35, comprising having the user entering the second password through the

data processing terminal ([0010-0018]).

As per Claim 36, the second password is entered automatically upon receipt of the first

password at the user's mobile communication terminal ([0070-0076]).

As per Claim 37, said first password is usable a limited number of times, or one time only

([0070-0076]).

As per Claim 38, comprising issuing to the user a second subscriber identity module

adapted to be used in the user's mobile communication terminal for authentication thereof in the

mobile communication network ([0010-0018]).

As per Claim 39, the second subscriber identity module has a fixed, one-to-one

relationship with the first subscriber identity module ([0070-0076]).

As per Claim 40, the first subscriber identity module is associated with an identifier of

the second subscriber identity module, or a mobile communication terminal number ([0070-

0096]).

As per Claim 41, said identification information is sent to the user's mobile communication terminal by way of a short message service message ([0070-0096]).

As per Claim 42, said first subscriber identity module is of a type adopted in mobile communication networks for authenticating mobile communication terminals ([0010-0018]).

As per Claim 43, said performing the first, SIM-based authentication of the data processing terminal comprises having the first subscriber identity module authenticated by an authentication server of the data processing system, the authentication server acting substantially as an authentication center of a mobile communication network operator ([0070-0096]).

As per Claim 45, in which the first subscriber identity module is of a type adopted in mobile communication networks for authenticating mobile communication terminals ([0010-0018]).

As per Claim 46, further comprising: retrieving SIM identification data from the first subscriber identity module ;communicating the retrieved SIM identification data to the authentication server, the authentication server acting substantially as an authentication center of a mobile communication network operator; receiving from the authentication server SIM authentication data corresponding to the SIM identification data, and passing the SIM identification data to the first subscriber identity module; and communicating to the authentication server a response generated by the first subscriber identity module ([0070-0096]).

As per Claim 47, a computer-readable medium encoded with a computer program product directly loadable into a working memory of a data processing terminal, the computer program product comprising software code portion capable of performing, when executed, the method according to claim 44 ([0054-0068]).

As per Claim 49, the first subscriber identity module is of a type adopted in mobile communication networks for authenticating mobile communication terminals, the authentication data processing server acting substantially as an authentication center of a mobile communication network operator ([0054-0068]).

As per Claim 50, further comprising: generating at the authentication data processing server a first password and sending the first password over the mobile communication network to the user's mobile communication terminal; and conditioning the authentication of the data processing terminal in the data processing system to a prescribed correspondence between the first password and a second password, depending on the first password, entered at the data processing terminal and provided to the authentication data processing server through the data processing system ([0058-0068]).

As per Claim 51, a computer-readable medium encoded with a computer program product directly loadable into a working memory of an authentication data processing system, the computer program product comprising software code portion capable of performing, when executed, the method according to claim 48 ([0054-0068]).

As per Claim 54, the first subscriber identity module is of a type adopted in mobile communication networks for authenticating mobile communication terminals ([0010-0018]).

As per Claim 55, comprising a second subscriber identity module to be used in the mobile communication terminal for authenticating the mobile communication terminal in a mobile communication network ([0010-0018]).

As per Claim 56, the second subscriber identity module is in a fixed, one-to-one relationship with the first subscriber identity module ([0070-0076]).

As per Claim 57, the second subscriber identity module is associated with an identifier of

the second subscriber identity module, particularly a mobile communication terminal number

([0070-0076]).

As per Claim 58, said first subscriber identity module is associated with a device

connectable to the computer through a computer peripheral connection port ([0010-0018]).

As per Claim 59, said mobile communication network is one among a GSM, a GPRS,

and a UMTS network ([0070-0096]).

As per Claim 61, the first subscriber identity module is of a type adopted in mobile

communication networks for authenticating mobile communication terminals ([0010-0018]).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
January 26, 2010
/Syed   Zia/
Primary Examiner, Art Unit 2431